NAVAL WAR COLLEGE
Newport, R.I.

OPERATIONAL PLANNING FUNCTIONS IN AN INFORMATION AGE

by

Joseph A. de Leon
Lieutenant Commander, USN

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: ______________________________

05 May 2001

7

REPORT DOCUMENTATION PAGE

1. Report Security Classification: UNCLASSIFIED

2. Security Classification Authority:

3. Declassification/Downgrading Schedule:

4. Distribution/Availability of Report: DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

5. Name of Performing Organization:

JOINT MILITARY OPERATIONS DEPARTMENT

6. Office Symbol: C

7. Address: NAVAL WAR COLLEGE
686 CUSHING ROAD
NEWPORT, RI 02841-1207

8. Title (Include Security Classification): OPERATIONAL PLANNING FUNCTIONS IN AN INFORMATION AGE (UNCLASSIFIED)

9. Personal Authors: LCDR Joseph A. de Leon, USN

10. Type of Report: FINAL

11. Date of Report: 05 May 2001

12. Page Count: 29 (includes notes and bibliography, pp20-28)

12A. Paper Advisor (if any):

13. Supplementary Notation: A paper submitted to the Faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. Ten key words that relate to your paper:

Operational Functions, NCW, Network-Centric Warfare, Operational Planning, Information Operations, Information Warfare, Information Age, decision making, Information Management, Knowledge-Based Warfare

15. Abstract:

Network Centric Warfare (NCW) as an emerging concept promises increased battle space awareness through information management. To the Operational Commander the potential for increased data collection and opportunities to capitalize on enemy information vulnerabilities provides greater opportunities for victory. The concept of Network Centric Warfare when coupled with technological advances and innovations will provide advantages through the Operational Planning Functions that will need to be considered during Joint Warfare planning. Compression of time, space and force factors will dictate a change in current command and control relationships and information management during the planning process and during the phases of conflict. The volume and speed of information networking will allow multi-plane command awareness and support the ability to mass effects on the battlefield. This will require the establishment of an Information planning function along with an Information Warfare Commander in the Joint Task Force structure.

16. Distribution / Availability of Abstract:	Unclassified X	Same As Rpt	DTIC Users

17. Abstract Security Classification: UNCLASSIFIED

18. Name of Responsible Individual: CHAIRMAN, JOINT MILITARY OPERATIONS DEPARTMENT

19. Telephone: 841-6461

20. Office Symbol: C

Security Classification of This Page Unclassified

LCDR J.A. DELEON, Seminar 7

Operational Planning Functions in an Information Age

Network Centric Warfare (NCW) as an emerging concept promises increased battle space awareness through information management. To the Operational Commander the potential for increased data collection and opportunities to capitalize on enemy information vulnerabilities provides greater opportunities for victory. The concept of Network Centric Warfare when coupled with technological advances and innovations will provide advantages through the Operational Planning Functions that will need to be considered during Joint Warfare planning. Compression of time, space and force factors will dictate a change in current command and control relationships and information management during the planning process and during the phases of conflict. The volume and speed of information networking will allow multi-plane command awareness and support the ability to mass effects on the battlefield. This will require the establishment of an Information planning function along with an Information Warfare Commander in the Joint Task Force structure.

As a corollary to the approach taken by Joseph W. Caneva in his 1999 Naval War College paper, "Network-Centric Warfare: Implications for Applying the Principles of War", this paper will focus on the impacts that NCW capabilities will have on the Operational Planning Functions of command and control, fires, intelligence, logistics and protection as applied to Joint Task Force Planning. An additional function focused on Information will be presented. The assumptions that speed and time compression will occur are accepted to be true for this analysis. The concepts presented here will not present Service specific programs currently in development nor will strategic implications of combined attacks through national power (i.e. combined informational and military) be addressed. With the current force structure and future posture it is assumed that most operations in the future will be Joint.

In all facets of society we can see how information has influenced all aspects of national power: Diplomatic, Informational, Military, Economic. The global economy affects our internal markets, and diplomatic concerns necessarily mirror economic concerns. The application of diplomatic power has been directly related to the support that is provided by the public. In recent years this has been greatly influenced by the "CNN factor" and other up to the minute news networks, including those based on the Internet. The public's ability to receive real-time information will continue to shape our national responses, be they diplomatic, economic, informational and military. In a recent film, Hollywood captured the potential impact of information in the recent James Bond movie, "Tomorrow Never Dies," the antagonist, Elliot Carver, a billionaire media mogul and certified terrorist, proclaimed satellites as his new artillery and his information/news as the ammunition. Through his manipulation of news-based perception he brought the world to the verge of a war through the manipulation of information by shaping the national perception and responses of China and the UK.[1]

Network Centric Warfare will become a force multiplier by "effective linking or networking of knowledgeable entities that are geographically or hierarchically dispersed."[2] The current accelerated cycle of technology has created an Information Revolution that will become the backbone of Network Centric Warfare. The basic building block of information technology, therefore, of Network Centric Warfare is the computer chip. A brief background on the dynamics of technological change and the computer chip evolution will provide an introductory understanding on the unstoppable transition to an information-based society.

The ability to increase the collection and processing of data with computer advances creates the information intensive environment required by NCW. Theoretically the next generation computer chip is introduced every eighteen months. This next generation involves both the complexities of the chip and the potential for miniaturization.[3] This cycle is expected to reach a zenith in the 2020 time frame due to the physical limitations in current microchip manufacturing when the capacity to etch transistors and wires onto silicon wafers will reach its upper limit. With these advances in computerization it will be possible to incorporate numerous sensors and computers into invisible networks that will assist people in everyday functions. In an industrial society example, the miniaturization of microprocessors, motors and servos have provided for numerous remote functions in an automobile; similarly miniature computers will network the functions in the "smart house" of tomorrow. [4]

In the concept of NCW innumerable networks will become nodes in the information management of both friendly and belligerent forces, societies, economies and nations. In conflict this will not be limited to only force related data. At the tactical and unit level computers imbedded in operating equipment will provide immediate reconfiguration for battle damage repairs as well as link the logistics requirements for maintenance, fuel, ammunition or replacement to the "network." This information then can be pulled into remote databases to identify real time requirements and tactical progress.

Information is the most critical product of NCW networks. Data is the fuel and the network is the engine through which command and control of this information generates usable knowledge. It had been assumed that an increase in the number of nodes increases battle space awareness and when applied properly Information Dominance can occur.

During this condition the enemy is denied the use of tactical data and the Commander has the advantage to select the optimal course of action to defeat the enemy. An analysis of the Operational Functions will show the dynamic changes required during the Information Revolution. Some studies project that the combination of leaps in technology and the ability to dominate the battlefield through information management will occur in the 2020-2050 time frame. Some of the implied impacts of NCW on current operational planning and the dynamics of required change will be discussed. These will necessarily impact the acceptance of future capabilities, highlight potential difficulties and support the Force After Next envisioned in Joint Vision 2020.

The concept of NCW will increase the information available for peacetime and wartime planning at the Operational Level. The James Bond scenario mentioned above is not beyond our current capabilities. Current miniaturization brings us the capability of global cellular phones, Internet connectable personal data assistants (PDA), and Global Positioning Systems (GPS) on wristwatches. This global technology already provides greater connectivity and tactical accuracy than was available to many combat forces during Operation Desert Storm. The Internet abounds with resources that range from weather satellite imagery, detailed maps and Internet phone connectivity. Satellite photography is available to the highest bidder and large bandwidth is commercially available. The resultant capabilities can become an instant intelligence infrastructure for would-be adversaries. "The growing use of computers and databases allows for the storage of vast amounts of information, much more than was previously possible on paper." [5] This rise in information volume can be called Information Intensity. Like the intensity of a storm, the ability to predict the result or harness the power of this information maelstrom may prove to be difficult but not impossible.

An accepted product of NCW is that its advantages will result in the compression of the operational factors of space and time. Through precision of synergized massed effects, force structure and requirements will likely decrease. In line with the current force reductions and initiatives towards lighter more mobile forces, these future forces if coupled with increased information awareness and massed effects will remain as capable if not more capable than equivalent forces today.[6] The net impact of NCW on the Operational Functions will be addressed in additional considerations for each function.

Fires

Operational Fires will undergo changes relevant to the objective and the capabilities of the enemy. Normally the End State of a conflict is achieved by attacking the enemy's critical vulnerabilities or center of gravity with force. Operational fires when applied properly have the effect of shaping the battlefield. NCW will offer the ability to conduct this shaping from great distances and irrespective of national borders and without placing soldiers at risk. In theory, Operational Fires in the information age will be directed at national and military information infrastructure that supports other operational functions such as logistics, intelligence and command and control. The application of electronic attack can result in significant degradation or paralysis of target systems. In some cases the mere threat of endangering these national or regional utilities and social frameworks may work to sway the popular support and political will of the belligerent. If war is an extension of politics, then non-lethal attack may lead to political decisions to avoid physical hostilities. In calendar year 2000, worldwide computer functions were affected by the "Love Bug" computer virus. This simple e-mail attachment originated in the Philippines and crippled economic and national systems both in the US and abroad. Millions of (defense, government, corporate and personal) computers were infected in the United States alone and numerous man-hours were consumed to purge the virus from vast networks.[7] A well-planned and precisely directed attack could result in significantly more paralysis of critical DOD Information systems.

Bridging the gap from the Strategic-Operational to Operational-Tactical application of Fires, informational attack will be directed at enemy command and control information networks. In much the same manner that strategic attack is conducted on national assets, directed military attacks will be conducted against information assets or forces in or supporting the operating area. With worldwide connectivity and global information access, supporting forces would not be required to be in the physical boundaries of the operational theater. Many data intensive and other supporting functions could easily be conducted by rear area forces that could be located anywhere in the world. These attack cells could be comprised of experts from any command in the national infrastructure. Through regional network operations these experts and skilled network warriors could conduct precision net-based operational fires that would preclude or precede an armed attack by networked combat forces. In theater, the ability to mass effects of fewer forces will provide precision fires that would potentially exceed the capabilities demonstrated in Desert Storm. Advanced weapons development will increase accuracy, reliability, survivability and lethality.

Movement and Maneuver

Movement and maneuver planning will be affected by the type of forces employed, physical (manned and unmanned) and informational. Current force downsizing and increased mobility initiatives put into motion by Joint Vision 2010 will evolve to support rapid maneuver capability with dispersed lines of communication. In the NCW Joint Operating Area (JOA), forces will be widely dispersed, massing only to achieve precise and decisive effects. Force on force maneuvers could be avoided. Today's strategy of a "show of force" by massing combat power will no longer be required. One of the strengths of NCW is its potential, within limits, to offset a disadvantage in numbers, technology or position.[8] Implied force and the threat of electronic force will represent national resolve and all aspects of national power. Combat forces will mass effects of ordnance and troops where required similar to the Marine Corps Operational Maneuver From the Sea (OMFTS) but in NCW from far beyond the horizon. Precision timing and information advantages will identify the precise targets to discourage counter attack or to disable national means of resistance. This will inherently create greater latitude for maneuver, which will provide maximum standoff and protection. Information forces will have the ability to attack across transnational borders, and combat forces (manned and unmanned) will only enter brief windows of vulnerability to conduct decisive precision attacks. Operational Maneuver From the Sea (OMFTS) and Ship to Objective Maneuver (STOM) and current operational concepts give examples of dispersed forces and precision attack. With limited assets traversing the battlefield, operational planning for force protection may decrease and we will see a greater emphasis in information operations defense. The survivability of the NCW infostructure will become a top priority.

Logistics

Operational Focused Logistics will see both benefits and pitfalls in a NCW environment. The push towards up-to-the-minute material status will generate vast amounts of data to be compiled and prioritized. Data submissions by smart ships, tanks, airplanes and even individual weapons will produce vast logistical databases. The resulting logistical requirements will have to be sorted and prioritized. Automated functions can assist in the information management but priorities will have to evolve with the dynamic tactical and operational pictures. Massed effects will not necessarily equate to precision logistics. Fewer combat forces may mean fewer requirements, but fewer assets will also mean fewer opportunities to deliver logistics support. In truth, much of the NCW concept hinges on developing technologies that may hold untapped efficiencies in fuel, weapons and physical sustainability for combat forces. However, Even unmanned assets will require maintenance and upkeep. Until these advances are introduced, traditional projections should remain applicable for initial combat sustainability for all forces and logistics planning will remain unchanged. The advances in networking will not necessarily

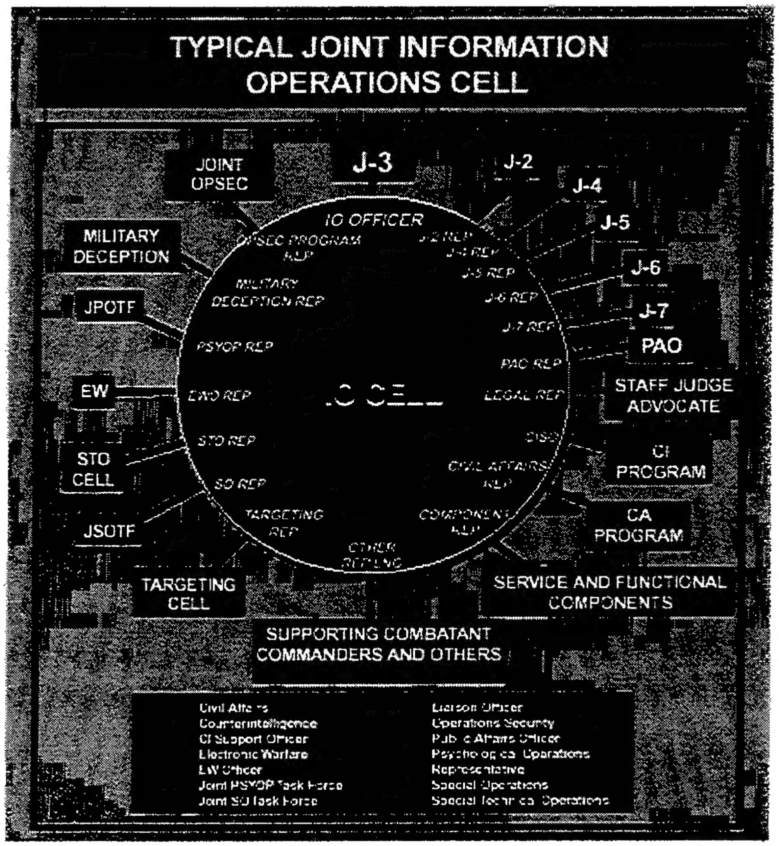

Figure 1 TYPICAL JOINT IO CELL (JOINT PUB 3-13)

equate to tomorrow's "just in time" logistics. As a benefit to operational planning dispersed forces may not require extended logistics lines of communication because they will deploy to the area to employ massed effects strikes and return to dispersed bases of operation and supply.

Intelligence

Operational Intelligence has become a subset of command and control as reflected in Joint Publication 3-13 which outlines the Information Operations (IO) cell (Figure 1). In most cases mission-defined intelligence objectives, limited national assets and time critical targeting will drive this cell's function. NCW holds the promise of real-time intelligence pushed down to the tactical level through technology-enhanced troops (the cyber-soldier) and machines. In a NCW force every combat unit will become a node in the network. In turn each node will be able to "pull" relevant information from the network to support mission accomplishment. Intelligence planning must factor in the number of nodes (i.e. troops, units, etc.) and determine priority of collection. If the wearable computer project at Massachusetts Institute of Technology's Media Lab is an indicator, every person can become a real-time information node on the World Wide Web. In this research lab, students have connected video output from an eyepiece to the Internet, sharing the video image with distant users.[9] Combine this capability with the U.S. Army's Land Warrior system where the soldier has a helmet eyepiece with access to a computer screen or weapons system video sight and you create a combat information node in every soldier.[10]

Infinite nodes could create an overwhelming information intensity that could degrade the network. Because of this intelligence volume, it might be beneficial if the intelligence cell complied the data into several key areas for assessment and dissemination by standing information and intelligence analysis cells. Dislocated intelligence assessment with real time feedback should be a goal. NCW connectivity would enable distant real time analysis of intelligence information with an unlimited array of products available to the Joint Task Force or regional Commander in Chief (CINC). This analysis could prioritize intelligence nodes on an individual level. Miniaturized components already exist that can create a precision targeting agent at the individual level. As stated in an earlier paragraph, Global Positioning System(GPS) is available on a wristwatch, point-to-point video is available on cellular phones, Internet connectivity is a personal data assistant (PDA) tap away. If technology advances in miniaturization continue, the "**Army of One**" may become a reality. With the ability to transmit real-time data from each combat unit (node), tactical intelligence will have a greater impact on the operational decision-making. The clarity, detail and precision based on emerging technologies will create virtual battle space awareness.

Command and Control

Command and control has two critical elements that will influence the application of NCW concepts in operations other than war and in armed conflict. The first of these is information management. Historically the management of information has paralleled the hierarchical command structure. In NCW, infinite connectivity has the potential to create a flatter information plane with horizontal vice vertical dissemination of critical decisions. However, the information begins as simple data and requires analysis before it becomes useful tactical or operational information. Input of this information into a common operational picture is required to provide both reference and relevance to any given situation. A significant yet ambiguous hurdle that will have to be cleared by the command and control decision makers is how best to manage the flow of information. "The critical weakness of both commercial and military domains, many of the basic technologies for simple sensor fusion are based on neural nets that are "trained" to recognize conditions in order to cue human intervention. These systems have a significant high false-positive rate and perform more poorly than skilled humans, although the amount of data analyzed is far greater."[11]

The second is information assessment. This is the process where information is turned into useful knowledge. The risk in this critical phase of command and control is that too much value might be placed on the efficiency and volume of information gathered. One viewpoint on information contends that,

> "Humans appear to be so versatile with respect to information use that human constraints or limitations are frequently ignored. Yet, asking users to define their information requirements will not necessarily yield a complete and correct set of requirements. Understanding the limitations of humans as information processors, human bias in selection and use of data, human problem-solving and the effects of background knowledge of the users will aid in overcoming process limitations."[12]

An analysis of the Marine Corps Sea Dragon Concept looked at automated decision aids with the following observations: 1) Applications designed to linearize the decision maker would try to create faster and better decisions through faster and better information. 2) Others would try to simplify the cognitive complexity of a problem by presenting the decision maker with integrated risk assessments. 3) Still others would attempt to predict the future through gaming and simulation of possible courses of action. While challenging, these changes would be going against the natural grain of the nonlinear decision making system.[13] Better decision-making does not arise from better information or more information. It is a result of careful analysis based on experience, training and better knowledge of the desired end state. The threat of NCW-based operations is a tendency to rely on the information to drive the decision, and not the converse where the information provides clarity to the correct decision.

Information

Information Operations (IO) are defined in Joint Publication 3-13 as "actions taken to affect adversary information and information systems while defending one's own..."[14] The focus of the current concept of information operations is on the operations of information collection, electronic warfare, IO system defense and offensive, civil affairs, public affairs and psychological operations. Unfortunately, this concept of information operations does not capture the vast potential of NCW-based operations, in particular the requirement to gather, process and disseminate vast amounts of data. The current concept consisting of an IO cell supporting the Joint Task Force Commander assumes that there exists a means to collect and process the infinite volume of information flowing into the "network" from infinite nodes.[15] Current Information Warfare doctrine is inadequate to cover the data management issues that will arise in NCW. Joint Pub 3-13 indicates that the "existing command and control warfare cell should be reconfigured to function as the IO cell."[16] This places the responsibility for IO planning on the J-3 in addition to planning current operations, which may not be optimal. This concept integrates current assets at hand into the J-3 information-planning cell, which includes intelligence resources, logistics, targeting, psychological operations (PSYOPS) and others (Figure 1). However, the current doctrine does not address the flow of data and the time required to produce tactically useful information.

The JTF staff requires an information "guru" or Information Commander that will act as the agent to manage the information flow and direct the collection of specified information (intelligence) with all assets available to support both operational and tactical objectives. The J-3 may be suited to prioritize the intelligence required to support mission accomplishment, however, a separate lead element should designate how that information is compiled. In addition to planning for information collection the Information Commander will be required to plan offensive and defensive IO and establish rule sets to control key databases critical to ongoing operations. This centralized control will ensure timely database update, authorized purging, and access. Many proponents of NCW envision a flatter plane of command and control that will be driven by the ability to pull information from infinite network nodes. In contrast to this, I see infinite date nodes and filters to control critical information flow. Command will remain a top down decision process with exceptions to time critical engagements. During war and operations other than war, the importance of controlling information at all levels is critical. "Shotgun" dissemination of a fire hose of information to all nodes (Department of Defense, Department of State, Non-Government Organizations, Private Volunteer Organizations, International Organizations, etc..) will run the inherent risk of vulnerability to the enemy. Even many of today's logistics information is transmitted over non-secure means, including the Internet. Security and access will always have to go hand in hand with IO.

The goal of both information management and assessment should be to achieve greater efficiency in command decision-making. Through increased speed of intelligence NCW will permit this process to proceed prior to the enemy's ability to react. Many parallel concepts exist to include, Knowledge Superiority, [17] Knowledge Based Warfare,[18] Informationalized War[19], and the broad term of Information Operations. NCW does not necessarily hinge on a flatter information and command structure that some theorize will be more efficient nor should the speed of intelligence and information require breakneck decision-making. Thomas Barnett, in his article, "The Seven Deadly Sins of NCW" argues that the information advantage, achieved in decisive time, will lengthen the decision loop thereby potentially improving the decision making process.[20] This approach to managing the information speed advantages may help preserve the hierarchical chain of command and the decision making value of the Commander. As in many instances, compressed and direct application of information is foreseen. In the case of time critical targeting, i.e. mobile targets, preplanned responses provide for command by negation. In contrast to the decentralized decision-making in a flatter command structure the practice of command by negation been successfully exercised in carrier battle group warfare organizations since the end of World War II. The Commander's Intent and specific/implied tasks should create the filter definitions that will assist in the meaningful analysis of data. The direction of weapons or weapons platforms from the foxhole is not the goal. Again, developing technologies will be critical in compressing the information-to-knowledge loop in order to support command decision-making.

Another concept in development to aid in the knowledge aspect of the decision loop is artificial intelligence based aids. "Intelligent agents" of the future based on artificial intelligence (AI) will act as filters, preventing us from drowning in an ocean of trivia and junk, enabling us to search for valuable information that we need.[21] The compression of time, space and force may require a compressed decision cycle in time-critical situations. However, the planning staff will have to promulgate specific guidelines and boundaries for AI based decision-making based on Operational Intelligence and Commander's Intent. The adjustment of these guidelines boundaries will have to occur continuously as variables enter the battle space, such as an emerging enemy capability. Some functions may be automated such as deployment of unmanned reconnaissance vehicles to refine information or preplanned weapons engagement if specific threat characteristics are displayed, similar to our current US Navy air defense systems.

Why should we be aggressively developing and implementing a NCW based concept today? We have entered a social period driven by global markets and information technology. The World Wide Web has enabled industries to respond to the real-time market and pursue research and development around the clock. Through the ability to export data a company is no longer bound by the 8-hour workday. Industries around the world already take advantage of this technological pace (the 24-hour day) to speed information based advances. For many military and State protection agencies this will equate to a 24/7/365 window of vulnerability from many peer competitors have developed concepts similar to NCW. This list can also include non-state terrorist groups and other anti-US organizations. "Technological superiority is not an absolute term. It is measured against a real or potential adversary's overall military capability."[22] If we look at our current near peer competitor, China, similar concepts on information warfare are held. Major General Wang Pufeng, the former Director of the Strategy Department at the Academy of Military Science, Beijing, stated that, "the flow of information, under the control of people, is injected into the flow of manpower, capacity, and materials, and will influence the form of warfare and determine victory or defeat. To achieve victory in information warfare, the central issue is control of information."[23] China has embraced the concept of Informationalized Warfare and admits to a technology lag behind the United States in developing supporting technologies.[24] However, the Chinese readily admit that a focus on weaknesses and the application of asymmetrical attacks can level the digital battlefield. A Rand Corporation analysis of future air operations stated, "It must be recognized that the adversary is a thinking, adapting, often highly motivated independent actor who will do creative and surprising things to counter U.S. sensors, weapons and innovative operations. Operations will have to be flexible to stay ahead and capitalize on discrete advantages."[25] With our nearest competitor pursuing NCW based capabilities, our closest allies however are having difficulties keeping pace with high tech developments in the U.S. Military.[26] If coalition involvement is to be assured in future conflicts then a sharing of technology and doctrine will be required. However, "the central problem of sharing knowledge is the impossibility of strictly limiting how partners will use knowledge gained from cooperation."[27] If capabilities cannot be matched, can true understanding of the network's information become a reality in coalition efforts? Or will we need to revert to "stove piped" information pushed to our coalition partners, thus losing the advantages of speed of information and the common operational picture NCW promises?

Because it is only a concept there can be an unlimited number of theories on the impact of NCW-based operations on operational planning. The Automated Battlefield, once a product of science fiction, is quickly becoming a reality. Technological advances have already led to unmanned vehicles, remote sensors, automated detection and classification. On the Automated Battlefields, computers would analyze sensor data and enemy forces would be engaged autonomously with precision weapons.[28] Will automation of the whole process of war eliminate planning in favor of programmed responses? Certainly this possibility is extreme at best. However a basic understanding of NCW may lead one to argue that operational planning as it exists today will not apply to future NCW based conflicts, that current operational functions are not adaptable to the asymmetrical attacks that our future enemies are planning. If we achieve the ability to cripple national and military infostructure, and our peer competitors achieve the same capability, then will our vulnerabilities prevent us from electronic forms of attack? This "mutually assured destruction" scenario via the electronic battlefield may create an information parity. Also, increasingly frequent operations other than war will involve our forces in areas of the globe where the infostructure to attack may not exist in sufficient depth to provide our forces an operational advantage through NCW.

In countries where the basic necessities are nonexistent, we will often be forced to revert to “boots on the ground” strategies in operations other that war? If an electronic vulnerability does not exist it cannot be attacked, then how will we leverage information technology? Will NCW drive force structure to the point where we cannot influence events by deployment of a credible force? Regardless, of the arguments, NCW is a concept that cannot be ignored with respect to the emergence of the Information Age. The risk lays in the inability to adapt to new forms of warfare and in the case of NCW the management of knowledge will be critical. NCW forces will provide precision capabilities that will enable US forces to win at the upper end of the spectrum of conflict. Its usefulness and application in operations other than war will necessarily be selective, but many vulnerabilities to IO will surface. As a recent example, Haiti, a country possessing no internal communications infrastructure, now has a thriving cellular phone market.[29] This country represents many countries that may require US intervention in operations other than war and which have made the first step into the information age. The availability of satellite-based connectivity and information technology can bring connectivity to any part of the world. For instance, Hybrid Network, Inc. is already working to provide continuous high-speed wireless Internet access to business and residential customers in the U.S. Virgin Islands.[30]

Network Centric Warfare remains as an emerging concept that parallels the transition of society from the industrial age to the information age. As illustrated in Figure 2, Information Operations occurs through all phases of the spectrum of conflict. NCW will enable the United States to compete at the upper end of the spectrum of conflict and provide advanced capabilities at all other levels. Technologically based capabilities which continue to develop will provide the operational commander the ability to harness vast amounts of information in both planning and execution phases of an operation. The impact of technology cannot be ignored and its by-products seen in all facets of society are: speed, capacity, flexibility, access, content, and DEMAND.[31] Yet developing technologies are still the linchpins on which many concepts such as NCW hinge. Although not yet in place, capabilities such as intelligent agents based on artificial intelligence in a short time will greatly add to the capability of knowledge management at the Joint Task Force staff level. The global network will provide access for the application of all forms of national power. If required this global connectivity will provide avenues for information-based deterrence, attack and, if needed, defense. In some concepts availability of data will break down the stovepipe approach to information management and allow critical users the ability to pull information as required from infinite sources. This ability is projected to result in greater force synergy and self-synchronization.

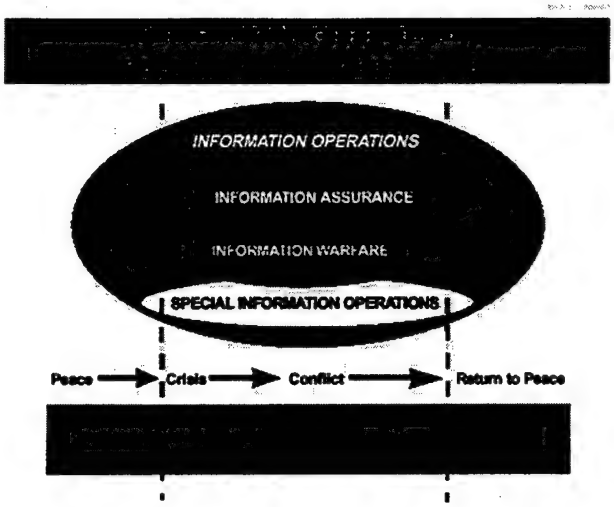

Figure 2 INFORMATION OPERATIONS RELATIONSHIPS ACROSS TIME (JOINT PUB 3-13)

In Mind the Gap, an analysis of Trans-Atlantic Revolution in Military Affairs, the authors summarized, "the advantage of being able to hit any target with any weapon from any platform, irrespective of range, armed service, or medium, argues for perfecting battlefield awareness, target detection, and weapon guidance. To meet such requirements, the successful application of information technology is important enough to justify major shifts in investment, doctrine and training. Absent such compelling needs the Revolution in Military Affairs (RMA) is mere gadgetry."[32] To paraphrase the Marine Corps perspective, Information Operations provides conceptually an integrating concept that will supplement the Operational Planning Functions not as an additional arrow in the Marine Air Ground Task Force Commander's quiver, but rather by "making the bow stronger."[33] The Commander is still the key element and his staff's planning is critical. Through the application of training, experience and judgment the knowledge gained through Network Centric Warfare the planning staff will have more capable tools to meet the Commander's Intent. Proper application of NCW advantages will ensure operations are planned to enable arrows fly true to their mark.

NOTES

[1] *Tomorrow Never Dies*, Metro Goldwin and Mayer, et al., 1997.

[2] David S. Alberts and others, Network Centric Warfare: Developing and Leveraging Information Superiority (Washington, CCRP, 1999), p6.

[3] Michio Kaku, Visions: How Science Will Revolutionize the 21st Century (New York, Anchor Books Doubleday, 1997), p29.

[4] Ibid.30. This limitation is the finite wavelength of light currently projected to be the pulsed excimer laser in the deep ultraviolet range (.193 micron). The current method uses mercury lamps, which enables etching to .365 microns (300 times thinner than a human hair.

[5] Robert A. Pitts and David Lei, Strategic Management: Building and Sustaining Competitive Advantage (USA, South-Western College Publishing, 2000), p443.

[6] Lawrence E. Casper, et al., "Knowledge-Based Warfare: A Security Strategy For The Next Century," Joint Forces Quarterly, Autumn 1996, 85.

[7] "FBI Launches Love Bug Inquiry," *BBC News Online:Sci/Tech*, 05 May 2000; <http://news.bnbc.co.uk/low/english/sci/tech/newsid_736000/736974.stm> accessed 12 January 2001.

[8] A. K. Cebrowski, et al., "Network-Centric Warfare: Its Origin and Future," U.S. Naval Institute Proceedings, January 1998, 32.

[9] Michio Kaku, Visions: How Science Will Revolutionize the 21st Century (New York, Anchor Books Doubleday, 1997), p35.

[10] Thomas K. Adams "The Real Military Revolution." Parameters. US Army War College Quarterly, Autumn 2000.

[11] Alan Vick, and others, Aerospace Operations In Urban Environments: Exploring New Concepts (Arlington, VA., RAND, 2000), p.183.

[12] Gordon B. Davis and Scott Hamilton, Managing Information: How Information Systems Impact Organizational Strategy (Homewood, ILL, Business One Irwin, 1993), p183.

[13] Robert R. Logan, LTCOL, USMC, "A Complex Dragon in a Chaotic Sea: New Science for USMC Information Age Decisionmakers," (Carlisle Barracks, PA. U.S. Army War College, 1996), p16

[14] Joint Chiefs of Staff, Joint Doctrine for Information Operations (Joint Pub 3-13)

(Washington, D.C.: October 9, 1998), vii.

[15] ibid, iv-3

[16] ibid

[17] Sharon Anderson, "Knowledge Based Management Leads to Knowledge Superiority, Interview with Dr. Robert E. Neilson, CHIPS Magazine Winter 2001, 7.

[18] Lawrence E. Casper, et al., "Knowledge-Based Warfare: A Security Strategy For The Next Century," Joint Forces Quarterly, Autumn 1996, 81.

[19] . Senior Colonel Wang Baocun and Li Fei, "Information Warfare," (excerpt from articles in Liberation Army Daily, June 13 and June 20 1995); <http://www.fas.org/irp/world/cina/docs/iw_wang.htm> accessed 22 January 2001.

[20] Thomas P.M. Barnett, "The Seven Deadly Sins of Network-Centric Warfare," U.S. Institute Proceedings, January 1999, 28-32.

[21] Michio Kaku, Visions: How Science Will Revolutionize the 21st Century (New York, Anchor Books Doubleday, 1997), p59.

[22] Peter M. Leitner, Decontrolling Strategic Technology, 1990-1992: Creating the Military Threats of the 21st Century (New York, University Press of America, 1995), p61.

[23] Major General Wang Pufeng, "The Challenge of Information Warfare," (excerpt from China Military Science , Spring 1995), <http://www.fas.org/irp/world/china/docs/iw_mg_wang.htm> accessed 22 January 2001.

[24] Senior Colonel Wang Baocun and Li Fei, "Information Warfare," (excerpt from articles in Liberation Army Daily, June 13 and June 20 1995); <http://www.fas.org/irp/world/china/docs/iw_wang.htm> accessed 22 January 2001.

[25] Alan Vick, and others, Aerospace Operations In Urban Environments: Exploring New Concepts (Arlington, VA., RAND, 2000), p.201.

[26] David C. Gompert, et al., Mind the Gap: Promoting A Transatlantic Revolution in Military Affairs (Washington, DC, National Defense Press, 1999), 9-16.

[27] Robert A. Pitts and David Lei, Strategic Management: Building and Sustaining Competative Advantage (USA, South-Western College Publishing, 2000), p280.

[28] John Tirman, The Militarization of High Technology (Cambridge, MA, Ballinger

Publishing Company, 1984), p53.

[29] Simon Romero, "Technology: A Cell Phone Surge Among World's Poor: In Haiti, Entrepreneurs as Suppliers," The New York Times, 19 December 2000.

[30] "Hybrid Networks to Supply Fixed Broadband Wireless Internet-Access System to Wireless World in U.S. Virgin Islands," PRNewswire, 10 January 2001, <http:/www.prnewswire.com>accessed on 02 February 2001 via AOL News Search at < aol://4344:30.L100ULXj.7230634.663600385>

[31]David S. Alperts, et al., "The Technologies of the Information Revolution," The Information Age: An Anthology on Its Impacts and Consequences Volume 1 Part One (Washington, DC, Natioanl Defense University, 1997), 107-111.

[32] David C. Gompert, et al., Mind the Gap: Promoting A Transatlantic Revolution in Military Affairs (Washington, DC, National Defense Press, 1999), 9.

[33] U.S. Marine Corps, United States Marine Corps Warfighting Concepts for the 21st Century (Quantico, VA, Marine Corps Development Command, 1998), ix-3.

BIBLIOGRAPHY

Adams, Thomas K. "The Real Military Revolution." Parameters. US Army War College Quarterly, Autumn 2000.

Alberts, David S. and John J. Garska, Frederick P Stein. Network Centric Warfare: Developing and Leveraging Information Superiority. Washington, D.C.: CCRP, 1999.

Anderson, Sharon. "Knowledge Based Management Leads to Knowledge Superiority." CHIPS Magazine, Winter 2001.

Aukofer, Frank and William P Lawrence, VADM, USN (Ret). America's Team; The Odd Couple-A Report on the Relationship Between the Media and the Military. Nashville, TN: The Freedom Forum First Amendment Center, 1995.

Baocun, Senior Colonel Wang and Li Fei, "Information Warfare," (excerpt from articles in Liberation Army Daily, June 13 and June 20 1995);<http://www.fas.org /irp/world/china/docs/iw_wang.htm> accessed 22 January 2001.

Barnett, Thomas P. M. "The Seven Deadly Sins of Network-Centric Warfare." U.S. Naval Institute Proceedings, January 1999.

Berkowitz, Bruce D. "Warfare in the Information Age." Information Age Anthology, VOL 1 Part Three, Government and Military. Washington, D.C.: National Defense University, June 1997, 519-544.

Blechman, Barry M. Technology and the Limitation of International Conflict. Washington D.C.: Foreign Policy Institute, 1989.

Borchert, R. Alistair, LCDR, USN, and Professor Carl R. Jones. "Organizational Fitness of a Proposed Network Centric Organization." Naval Post Graduate School Monterey California. CCRP/1999 Command and Control, Research and Technology Symposium Publication VOL 2 Track 4: Information Technology, June 1999, 781-813.

Boyd, Richard K., "A Weapons Systems Development Decision Support System." DTIC/Naval Postgraduate School Monterey, California Technical Report, March 1992.

Campbell, John, "Information Technology, Friend or Foe of Command and Control." J.C. Consulting (UK) Ltd. CCRP/1999 Command and Control, Research and Technology Symposium publication, VOL 2 Track 4: Information Technology, June 1999.

Caneva, Joseph W., "Network-Centric Warfare: Implications for Applying the Principles of War." Naval War College Research Paper. Naval War College, Newport, Rhode Island, 1999.

Casper, Lawrence E. et al. "Knowledge-Based Warfare: A Security Strategy For The Next Century." Joint Forces Quarterly, Autumn 1996.

Cebrowski, Arthur K., VADM, USN and John J. Garstka. "Network-Centric Warfare—Its Origin and Future." U.S. Naval Institute Proceedings, January 1998, 28-35.

Cebrowski, Arthur K., VADM, USN, "Network Centric Warfare: An Emerging Military Response to the Information Age." Presentation given on 29 June 1999 at the 1999 Command and Control, Research and Technology Symposium.

Chief of Naval Operations. Naval Intelligence (Naval Doctrine Publication 2). Washington, D.C., 1995.

Chief of Naval Operations. Naval Command and Control (Naval Doctrine Publication 6). Washington, D.C., 1995.

Crow, Michael and Barry Bozeman. Limited By Design: R&D Laboratories in the U.S. National Innovation System. New York: Columbia University Press, 1998.

CSIS, Center for Strategic and International Studies. "Integrating Commercial and Military Technologies for National Strength: An Agenda for Change." CSIS, January 1991.

Davis, Gordon B. and Scott Hamilton. Managing Information. Homewood, Illinois, Business One Irvine, 1993.

De Simone, Daniel V. Education for Innovation. Oxford, England: Pergamon Press, 1968.

DTIC Review. "Future Directions: Preparing for the 21st Century (Collection of 4 Documents)" Fort Belvoir, Virginia: DTIC, July 1996.

"FBI Launches Love Bug Inquiry," *BBC News Online:Sci/Tech*, 05 May 2000; <http://news.bnbc.co.uk/low/english/sci/tech/newsid_736000 /736974.stm> accessed 12 January 2001.

Gillam, Mary M., Major. "Information Warfare: Combating The Threat In The 21st Century." Unpublished research paper, Air Command and Staff College, March 1997.

Gompert, David C. Mind the Gap: Promoting A Transatlantic Revolution in Military Affairs. Washington, D.C.: National Defense Press, 1999.

Guthrei, Samuel A., MAJ USA. "Knowledge-Based Operations: The "So What" of Information Warfare. Fort Levenworth, Kansas: US Army Command and General Staff College. DTIC Technical Report, 1995.

Hall, Wayne M., Brigadier General, USA (Ret). "Information Operations (IO): Military Competition." Cyber Sword, Fall 2000.

Hellman, Hal. Technophobia: Getting out of the TechnologyTrap. New York M: Evans and Company, Inc, 1976.

Helms, Chet, CAPT, USN. "Operational Factors." Joint Military Operations Department Reading NWC 40922A, Naval War College, Newport, Rhode Island.

Helms, Chet, CAPT, USN. "Operational Functions." Joint Military Operations Department Reading NWC 4103A, Naval War College, Newport Rhode Island.

Hunt, Geoffrey H., Lt. Col. UK. "The Development of the United Kingdom's Single Army Activity Model and Associated Information Needs and It's Relationship to Command and Control." UK Ministry of Defense. CCRP/1999 Command and Control, Research and Technology Symposium Publication, VOL 2 Track 4: Information Technology, June 1999, 814-856.

"Hybrid Networks to Supply Fixed Broadband Wireless Internet-Access System to Wireless World in U.S. Virgin Islands," PRNewswire, 10 January 2001, <http:/www.prnewswire.com>accessed on 02 February 2001 via AOL News Search at < aol://4344:30.L100ULXj.7230634.663600385>

Jedryski, Peter A. "The Interactive Data Wall." Air Force Research Laboratory/IFSA. CCRP/1999 Command and Control, Research and Technology Symposium Publication VOL 2 Track 4: Information Technology, June 1999, 955-970.

Kaku, Michio. Visions: How Science Will Revolutionize the Twenty-first Century. New York: Anchor Books Doubleday, 1997.

Kamradt, Henry and Douglas MacDonald, CDR, RN. "The Implications of Network-Centric Warfare for the United States and Multinational Military Operations. U.S. Naval War College Decision Support Department Occasional Paper 98-1, 31 December 1998.

Kasten, George, CAPT, USN. "Building A Beehive: Observations on the Transition to Network-Centric Operations." Naval War College, Strategic Research Department. 3 May 2000. <http:// nwcintranet/intranetsearch/srd/publications /beehive/beehive03may.htm>

Kempis, Rolf-Dieter and Jurgen Ringbeck. Do It Smart: Seven Rules for Superior Informaiton Technology Performance. New York: The Free Press, 1988.

Leary, W.H., III. "Corporate Information Management for the 21st Century." Fort Belvoir, Virginia: DTIC, June 1994.

Leitner, Peter M. Decontrolling Strategic Technology, 1990-1992: Creating the Military Threats of the 21st Century. Lanham, Maryland: University Press of America, 1995.

Liang, Qiao and Wang Xiangsui. Unrestricted Warfare. Beijing: Literature Arts Publishing House, 1999.

Logan, Robert R, LCOL, USMC. "A Complex Dragon in a Chaotic Sea: New Science for USMC Information Age Decisionmakers." DTIC/Carlisle Barracks, U.S. Army War College, January 1996.

Naval War College Faculty, "Network Centric Operations: A Capstone Concept for Naval Operations in the Information Age (draft)." Naval War College, Newport, Rhode Island.

OECD. The Conditions for Success in Technological Innovation. Paris: Organisation for Economic Co-Operation and Development, 1971.

Owens, Donald G. "Underpinning the RMA - Advancements in the Transformation of Information into Knowledge for Command and Control." CCRP C4ISR Battle Center /1999 Command and Control, Research and Technology Symposium Publication VOL 2 Track 4: Information Technology, June 1999, 856-870.

Pitts, Robert A. and David Lei. Strategic Management: Building and Sustaining Competitive Advantage. USA: Southwestern College Publishing, 2000.

Postman, Niel. Technopoly: The Surrender of Culture to Technology. New York: Vintage Books, 1992.

Pufeng, Major General Wang . "The Challenge of Information Warfare," (excerpt from China Military Science , Spring 1995), <http://www.fas.org/irp/world /china/docs/iw_mg_wang.htm> accessed 22 January 2001.

Romero, Simon, "Technology: A Cell Phone Surge Among World's Poor: In Haiti, Entrepreneurs as Suppliers," The New York Times, 19 December 2000.

Sarkar, Susan and Paul Richardson. "Distributed Computations in the Digitized Battlefield." VETRONICS Laboratory, US Army, CCRP/1999 Command and Control, Research and Technology Symposium Publication VOL 2 Track 4: Information Technology, June 1999.

Schnell, David Allan. "Stormy Waters: Technology, Sea Control and Regional Warfare." Unpublished Student Research Paper. Naval Postgraduate School, Monterey, California. June 1994.

Sengupta, Kishore and Carl R. Jones. "Creating Structures for Network-Centric Warfare: Perspectives from Organization Theory." Naval Post Graduate School, Monterey, California, CCRP/1999 Command and Control, Research and Technology Symposium Publication VOL 2 Track 4: Information Technology, June 1999.

Storr, J.P., Maj (UK). "Alternative Concepts for Battlefield Command and Control Organizations." UK Ministry of Defense, CCRP/1999 Command and Control, Research and Technology Symposium Publication VOL 2 Track 4: Information Technology, June 1999.

Strickland, Frank B. "It's Not About Mousetraps-Measuring the Value of Knowledge for Operators." Joint Forces Quarterly, Autumn 1996.

Swain, George S. "Understanding the Organizational Decision Process at the Theater Commander-in-Chief Level of Command." DTIC/Naval Postgraduate School. Fort Belvoir, Virginia: DTIC Technical Report, March 1990.

Teich, Albert H. Technology and the Future. New York: St. Martin's Press, 1990.

Tirman, John. The Militarization of High Technology. Cambridge, Massachusetts: Ballinger Publishing Company, 1984.

U.S. Joint Chiefs of Staff. Doctrine for Intelligence Support to Joint Operations (Joint Pub 2-0). Washington, D.C., 2000.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations (Joint Pub 3-13). Washington, D.C., 1998.

U.S. Joint Chiefs of Staff. Doctrine for Logistics Support of Joint Operations (Joint Pub 4-0). Washington, D.C., 2000.

U.S. Joint Chiefs of Staff. Joint Vision 2010. Washington, D.C. not dated.

U.S. Joint Chiefs of Staff. Joint Vision 2020. Washington, DC. not dated.

United Artists. *Tomorrow Never Dies.* 1997.

United States Marine Corps Combat Development Command, Concepts Division. United States Marine Corps Warfighting Concepts for the 21st Century. Quantico, Virginia, not dated.

Vick, Stillion, Frelinger, Kvitky, Lambeth, Amrquis, Waxman. Aerospace Operations in Urban Environments: Exploring New Technologies. Arlington, Virginia: USAF/RAND, 2000.

Waldrop, M. Mitchell. Complexity: The Emerging Science at the Edge of Order and Chaos. New York: Touchstone Books, 1992.

The White House. A National Security Strategy for the Next Century. December 1999.

Zimm, Alan D., CDR, USN (Ret). "Human Centric Warfare." U.S. Naval Institute Proceedings, May 1999.